PATENT
PD-00-1016

CHAOTIC PRIVACY SYSTEM AND METHOD

Richard H. Sherman
Chamroeun Kchao
Billy Pettijohn

CHAOTIC PRIVACY SYSTEM AND METHOD

BACKGROUND

The present invention relates generally to privacy systems and methods, and more particularly, to improved chaotic privacy systems and methods.

Traditionally privacy for analog signals is established by digitizing the signals, then encrypting bits of the signal with a secure algorithm, which then generates a digital signal for transmission, or the digital signal is reconverted back to an analog signal. The sampling process is error prone with sampling error, quantizing error and losses due to a bandlimited channel. If the original analog signal is desired, then the received digital signal could be passed through a digital-to-analog converter to recover the analog signal.

Examples of this process include secure speech and secure video. For analog signals of high bandwidth, the sampling process is even more error prone due to technology limitations of analog-to-digital converters. For example, a 4 GHz bandwidth with a 10 giga-sample per second sample rate, each sample with 8 bits per sample, requires a transmission bit rate of 80 giga-bits per second. Neither the analog-to-digital conversion nor the free space transmission bandwidth are possible with currently-available technology.

Analog privacy involves information secrecy where the information is concealed by a cipher or a code. The existence of a message is not hidden, only its information content. An unintended receiver is assumed to have the required equipment necessary to intercept and record the transmitted signal. The interceptor may even know the structure of the transmitter and receiver.

In Shannon Secrecy, the probability density of transmitted signal is independent from the information signal probability density. One way to achieve this independence is to cause the transmitted signal to have nearly an nth order uniform density distribution. The inverse function, which recovers the information, would require a key parameter without which no information can be recovered.

The other traditional approach for protecting analog signals is spread spectrum and/or frequency hopping techniques. The spread spectrum techniques use a pseudorandom noise generator with a reproducible number sequence in the receiver. These techniques have a pseudo random repetition period , which can be used to break the disguised signal.

It is therefore an objective of the present invention to provide for chaotic privacy systems and methods that protect analog signals and improve upon the above-discussed techniques.

SUMMARY OF THE INVENTION

To accomplish the above and other objectives, the present invention provides for chaotic privacy systems and methods that protect analog signals transmitted from a transmitter to a receiver. The approach used in the chaotic privacy systems and methods is to use a chaotic circuit as a random signal generator for a key stream. Unlike spread spectrum techniques, there is no pseudorandom repetition period. In the transmitter, a function, f(.,.), of two variables is used to operate on information signals i(t) and a key stream, k(t). The function is designed to preserve a cipherwave, c(t), as a uniform probability density for all information signals i(t) and key streams k(t).

In the receiver, chaotic circuit synchronization reproduces a copy of the random signal. This synchronization occurs for each element of f(.,k). The cipherwave preserves the nth order uniform distribution of the cipherwave c(t). A key generator is defined by $i_k(.)$. A key parameter, z(0), is used to define the key generator dynamics. Unless the receiver possess the key parameter, it will not synchronize,

The present invention protects analog signals such that an unintended receiver cannot recover the analog information or recognize the pattern of the analog information contained in the transmitted signal. The present invention transmits a secure random signal that is synchronized with an intended receiver using synchronized chaos. In the present invention, protection comes through the use of a Shannon Secrecy argument applied to the analog information signals that are transmitted. The chaotic circuits used in the present invention are synchronized for data recovery without sampling the transmitted information signal.

One advantage of the present chaotic privacy systems and methods is that there are no periodic components. The chaotic privacy systems and methods do not require sampling or channelizing the bandlimited analog information signal.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of the present invention may be more readily understood with reference to the following detailed description taken in conjunction with the accompanying drawings, wherein like reference numerals designate like structural element, and in which:

Fig. 1 illustrates the architecture of an exemplary chaos privacy system in accordance with the principles of the present invention;

Fig. 2 illustrates mutual information loss as a function of iteration for the random number generator used in the present invention;

Fig. 3 illustrates that the architecture of the key generator used in the present invention is a chaotic circuit;

Fig. 4 illustrates that the input and output of the key generator are defined by the sampled value;

Fig. 5 illustrates details of the transmitter of the system shown in Fig. 1, which uses coupled digital phase lock loops;

Fig. 6 illustrates details of the receiver of the system shown in Fig. 1, which contains a copy of the digital phase lock loop used in the transmitter, and reproduces the key stream; and

Fig. 7 is a flow diagram illustrating an exemplary chaos privacy method in accordance with the principles of the present invention.

DETAILED DESCRIPTION

Referring to the drawing figures, Fig. 1 illustrates the architecture of an exemplary chaos privacy system 10 in accordance with the principles of the present invention. The exemplary chaos privacy system 10 comprises a transmitter 20 and a receiver 30. Information signals are communicated by way of a communication channel from the transmitter 20 to the receiver 30.

The transmitter 20 comprises a key stream generator 21 and a transmitting chaotic circuit 22. The key stream generator 21 generates a key stream k(t) in response to a private key parameter z(0), The key stream generator 21 also outputs a key synchronization parameter (or public key) u*(t) which is transmitted to the receiver 30 by way of the communication channel. The transmitting chaotic circuit 22 processes a band limited analog information signal i(t) and the key stream k(t) output by the key

stream generator 21, and outputs a cipherwave c(t) which is a function f(.,.) of the analog information signal i(t) and the key stream. The cipherwave c(t) is transmitted to the receiver 30 by way of the communication channel.

The receiver 30 comprises a key stream generator 31 and a receiving chaotic circuit 32. The receiving chaotic circuit 32 processes a copy of the private key parameter z*(0) and the key synchronization parameter (or public key) u*(t) transmitted from the key stream generator 21 in the transmitter 20. The receiving chaotic circuit 32 generates a copy of the key stream k*(t). The receiving chaotic circuit 32 processes the copy of the key stream k*(t) and the cipherwave c(t), and demodulates the cipherwave c(t) to recover and output the analog information signal, i*(t).

The system 10 thus provides privacy in transmitting the analog information signal. The system 10 combines the information signal with the analog random signal generated by the transmitting chaotic circuit 22 that is synchronized with the receiving chaotic circuit 32. The received signal is demodulated using a synchronized replica of the analog random signal. The information signal is recovered since the product of the random signals, one generated in the transmitter 20 and one generated in the receiver 30, is unity.

The security of the random number generator (key stream generator 21), and particularly repeatable generators, is of importance in security. The security of a random number generator means, how difficult it is, based on past values of a sequence, to predict future values of the sequence. One measure of the difficulty is in information theory terms. The lower the mutual information between the present state and a previous state, the more difficult it is to recover the previous state.

The average rate of information loss in a chaotic system is equal to the Lyapunov exponent. The Lyapunov exponent may be calculated from the invariant probability distribution:

$$\lambda = \int_0^{2\pi} \log\left|\frac{df}{d\phi}\right| \bullet p(\phi)d\phi .$$

The above probability distribution gives the information loss for the nonlinear circuit (key stream generator 21) used to generate random numbers in the system 10. Fig. 2 is a plot that illustrates mutual information loss as a function of iteration for the random number generator (key stream generator 21). Each iteration is a separate frequency generated by the system 10 using the plot illustrated in Fig 2.

Chaotic circuits.

Details of exemplary random number generators (key stream generators 21, 31) employed in the system 10 are illustrated in Fig. 3. The random number generators may be represented mathematically as a Sine circle map, given by the equations

fn = tn mod 1, and

fn+1 = fn + 1/(fo(1+b sin(2p tn)).

There are two parameters, that characterize the dynamics of the random number generators: fo, which is the initial phase angle, and b, which is the loop gain.

Fig. 3 illustrates that the architecture of the key stream generators 21, 31 used in the system 10 are chaotic circuits. A signal having frequency components (generated by a separate voltage controlled oscillator) is sampled by a sample and hold circuit (S&H) 41. The analog sample values are used as control voltages for a voltage controlled oscillator (VCO) 42. The frequencies of the signals output by the VCO 42 are centered around zero. The output signals from the VCO 42 (random keys or key stream) are input to an RF correlation device 43 that correlates them with the information signal i(t). When an output wave crosses the zero axis, a signal is sent to the sample and hold circuit 41 to acquire the next sample. The process repeats, but each time a different sample value is acquired, and a different frequency results. The output of the RF correlation device 43 is a slightly spread encoded signal s(t).

Fig. 4 illustrates that the input and output of the key stream generator 21 are defined by the sampled value. Fig. 4 illustrates several periods of operation. Each period results in a voltage (shown on the right side of Fig. 4) and an output frequency (shown on the bottom of Fig. 4). The loop gain parameter, b, controls the frequency resulting from the sampled value.

Fig. 5 illustrates details of the transmitter 20 of the system 10 shown in Fig. 1, which uses first and second coupled digital phase lock loops (DPLL1, DPLL2) 51, 52. The transmitter 20 thus includes a pair of coupled chaotic circuits comprising the two digital phase lock loops 51, 52. The first digital phase lock loop 51 comprises a sample and hold circuit 41 coupled to a voltage controlled oscillator 42 in the manner discussed with reference to Fig. 3. The second digital phase lock loop 52 also comprises a sample and hold circuit (41 coupled to a voltage controlled oscillator 42.

The VCO 42 in the first digital phase lock loop 51 receives a first loop gain signal b1 while the VCO 42 in the second digital phase lock loop 52 receives a second loop gain signal b2. The output of the VCO 42 in the first digital phase lock loop 51 is input to the sample and hold circuit 41 of the second digital phase lock loop 52. The output of the VCO 42 in the second digital phase lock loop 52 is input to the sample and hold circuit 41 of the first digital phase lock loop 51. The VCO 42 samples the signal in the associated sample and hold circuit 41 and generates an output frequency in response thereto.

The output of the VCO 42 in the first digital phase lock loop 51 is converted to +1 or –1 by a hard limiting circuit 53, and is input to an analog multiplier circuit 54.

The product of the information signal, i(t) and the sampled random signal output by the hard limiting circuit 53 is the cipherwave c(t). The multiplication performed by the analog multiplier circuit 54 spreads the information signal spectrum. For example, the information signal bandwidth could be 500 MHz, and the frequency "fo" could be at 375 MHz. This yields a spreading factor of less than 1.7 between the information signal and the cipherwave c(t).

The purpose of the coupled chaotic circuits (the first and second coupled digital phase lock loops 51, 52) is to allow synchronization with a third chaotic circuit 61 located in the receiver 30. The purpose of the hard limiting circuit 53 is to insure that the multiplier product does not attenuate any information signal components.

Fig. 6 illustrates details of the receiver 30 of the system 10 shown in Fig. 1, which contains the third chaotic circuit 61 which is a copy of the first digital phase lock loop 51 used in the transmitter 20, and reproduces the key stream. The receiver 30 is similar to the transmitter 20. The receiver 30 comprises a pair of coupled chaotic circuits comprising the third and fourth digital phase lock loops (DPLL3, DPLL4) 61, 62.

The third digital phase lock loop 61 comprises a sample and hold circuit 41 coupled to a voltage controlled oscillator 42. The fourth digital phase lock loop 62 also comprises a sample and hold circuit 41 coupled to a voltage controlled oscillator 42.

The VCO 42 in the third digital phase lock loop 61 receives the first loop gain signal b1 while the VCO 42 in the fourth digital phase lock loop 62 receives the second loop gain signal b2. The output of the VCO 42 in the third digital phase lock loop 61 is input to the sample and hold circuit 41 of the fourth digital phase lock loop 62. The output of the VCO 42 in the fourth digital phase lock loop 62 is input to the sample and hold circuit 41 of the third digital phase lock loop 61. The VCO 42 samples the signal in the associated sample and hold circuit 41 and generates an output frequency in response thereto.

An input switch 66 is provided at the public key input to the third digital phase lock loop 61. The output of the VCO 42 in the third digital phase lock loop 61 is converted to +1 or –1 by a hard limiting circuit 63, is input to the analog multiplier circuit 65.

The information signal i*(t) is reconstructed from the cipherwave, c(t) by multiplying by a repeatable random number in the analog multiplier circuit 65. Since the product of -1*-1 and 1*1 both equal 1, the randomness is removed.

The third digital phase lock loop 61 synchronizes to the chaotic circuits 51, 52 in the transmitter 20 because it is a copy of the first digital phase lock loop 51 with the same input signals. The purpose of the input switch 66 and the fourth digital phase lock

loop 62 is to reduce the data rate needed for the public channel. The purpose of the fourth digital phase lock loop 62 is to copy the actions of the second digital phase lock loop 52.

When the input switch 66 is closed, then the third digital phase lock loop 61 receives the same input as the first digital phase lock loop 51. When the input switch 66 is open, then the third digital phase lock loop 61 receives a similar input using the fourth digital phase lock loop 62.

The number of samples that may be discarded is a function of the degree of synchronization at the key parameter values. If a digital channel is used for the public key, an A/D and D/A converter would be used with the sampling frequency, fo.

There are an infinite number of possible key parameters that provide chaos and that provide synchronization. A plot of normalized phase angle versus key parameter, b, reveals this. Any value of the key parameter, b, between 140 and 200 provides for a chaotic signal output.

Referring now to Fig. 7, it is a flow diagram illustrating an exemplary chaos privacy method 70 in accordance with the principles of the present invention. The exemplary chaos privacy method 70 comprises the following steps.

A random key stream k(t) is generated 71 using a chaotic circuit. Analog information signals i(t) and the random key stream k(t) are processed 72 to generate a cipherwave c(t) that has a uniform probability density for all information signals i(t), and random key streams k(t). The cipherwave c(t) and a public key k(t) are transmitted 73 over a communication channel. The cipherwave c(t) and public key k(t) are received 74. A chaotic circuit is used to synchronize 75 to the public key k(t) to produce a copy of the random key stream k*(t). The cipherwave c(t) and the copy of the random key stream k*(t) are processed 76 to reconstruct the information signal i*(t).

Thus chaotic privacy systems and methods have been disclosed. It is to be understood that the above-described embodiments are merely illustrative of some of the many specific embodiments that represent applications of the principles of the present invention. Clearly, numerous and other arrangements can be readily devised by those skilled in the art without departing from the scope of the invention.